THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>PAIGE THOMPSON,<br><br>Defendant. | No. CR19-159-RSL<br><br>**MOTION TO STRIKE THE CRYPTO MINING ALLEGATIONS OF COUNT ONE AND TO SEVER COUNT EIGHT OF THE INDICTMENT**<br><br>Noted for January 14, 2022 |

## I. INTRODUCTION

Defendant Paige Thompson, through counsel, files this motion to strike the crypto mining allegations of Count 1, which charges wire fraud, and to sever Count 8, which charges unauthorized access to computers for crypto mining. Count 1 contains two vague and unrelated theories of wire fraud liability. The first theory alleges that Ms. Thompson stole information from entities that leased computers from AWS as part of a scheme to defraud when she accessed computers without authorization. The second alleged theory is that she used computers belonging to AWS to mine for cryptocurrency. The Court should not permit the government to offer the second theory—the crypto mining allegations—at trial because doing so will impermissibly prejudice Ms. Thompson in contravention of Federal Rules of Criminal Procedure 7(d). Those allegations should be struck.

/ / /

/ / /



**FEDERAL PUBLIC DEFENDER**
**1601 Fifth Avenue, Suite 700**
**Seattle, WA 98101**
**(206) 553-1100**

For the same reasons that the Court should strike Count 1's crypto mining allegations, the Court also should sever Count 8, which relates to crypto mining. Its inclusion will confuse the jury in violation of Federal Rule of Criminal Procedure 14(a). At a minimum, the Court should hold an evidentiary hearing to determine whether severance of Count 8 from the remaining counts in the Indictment is appropriate.

## II. RELEVANT FACTS

On June 17, 2021, the grand jury returned a superseding indictment ("Indictment"), which included ten counts.[1] Dkt. No. 102.

### A. The Wire Fraud Theories (Count 1)

Count 1, which charges Ms. Thompson with wire fraud in violation of 18 U.S.C. § 1343, alleges two distinct schemes to defraud the alleged victims. *Id.* at 3. In the first alleged scheme, Ms. Thompson "exploit[ed] the fact that certain customers of [AWS] had misconfigured web application firewalls" with the object of "us[ing] that misconfiguration to obtain credentials for accounts of those customers . . . to view and copy data stored by the customers." *Id.* The Indictment also alleges a second scheme in which Ms. Thompson exploited the misconfigured web application firewalls in order to use the accessed servers to mine cryptocurrency. *Id.*

Count 1 identifies eight alleged victims—Capita1 (Victim 1), an "agency of a state" (Victim 2), an unidentified foreign "telecommunications conglomerate" (Victim 3), an unidentified public research university (Victim 4), an unidentified "technology company that specializes in digital rights management" (Victim 5), an unidentified "technology company that provides data and threat protection services" (Victim 6), an unidentified "technology company that provides interaction-management solutions" (Victim 7), and an unidentified "technology company that provides higher education

[1] The original indictment was filed on August 28, 2019, and included two counts charging wire fraud (Count 1) and violation of the Computer Fraud and Abuse Act (Count 2). Dkt. No. 33.



**FEDERAL PUBLIC DEFENDER**
**1601 Fifth Avenue, Suite 700**
**Seattle, WA 98101**
**(206) 553-1100**

learning technology" (Victim 8)—though it does not allege with specificity which victims were subject to which alleged scheme. *Id.* at 2-3. Indeed, the *only* specifics the Indictment provides are with respect to data allegedly "stole[n]" from Capital One. *Id.* at 4-5. Count 1 lacks *any* allegation that Ms. Thompson attempted to monetize or profit from the alleged copying of stored data in any way whatsoever.

**B. The CFAA Theories (Counts 2-8)**

Counts 2-8 charge Ms. Thompson with violations of the Computer Fraud and Abuse Act (the "CFAA"). Specifically, it is alleged that she accessed the rented AWS servers of various victims without authorization for the purpose of furthering the two distinct schemes as alleged in Count 1. Counts 2-7 allege that Ms. Thompson accessed computers without authorization to view and take stored data from Capital One (Victim 1) and telecommunications company (Victims 3) and (Victims 5-8), while Count 8 alleges that she accessed the computers of "Victim 7, Victim 8, and other victims" without authorization to "perform cryptocurrency mining." *Id.* at 5-8. (Victim 2) the state agency and (Victim 4) a public research university are not mentioned anywhere in the CFAA counts. The Indictment does not make it clear if they are part of the "other victims" alleged in Count 8.

None of the CFAA counts specify the stored data allegedly taken or its value, nor does Count 8 articulate with specificity the type of cryptocurrency mining in which Ms. Thompson purportedly engaged (*i.e.,* BTC, ETH, an altcoin, etc.) nor the amount of cryptocurrency she allegedly mined as a result of her alleged activities. Notably, the government did not seize any fiat money or cryptocurrency in this matter. The Indictment also appears to be aggregating alleged losses under Count 8, in which it alleges over $5,000 in loss, but then it refers to multiple victims without identifying all of them. *Id.* at 7.



**FEDERAL PUBLIC DEFENDER**
**1601 Fifth Avenue, Suite 700**
**Seattle, WA 98101**
**(206) 553-1100**

## III. LEGAL ANALYSIS

### A. The Court Should Strike the Surplus Crypto Mining Allegations From Count 1 Pursuant to Fed. R. Crim. P. 7(d) Because They Are Both Collateral and Impermissibly Prejudicial.

The Court should exercise its discretion and strike the crypto mining allegations from Count 1, which are contained only in Paragraph 21. Pursuant to Federal Rule of Criminal Procedure 7(d), a defendant may move the court to "strike surplusage from the indictment or information" to "protect a defendant against prejudicial or inflammatory allegations that are neither relevant nor material to the charges." *United States v. Laurienti*, 611 F.3d 530, 546-47 (9th Cir. 2010) (*quoting United States v. Terrigno*, 838 F.2d 371, 373 (9th Cir. 1988)); *see United States v. Payne*, No. 216CR00046GMNPAL, 2017 WL 68616, at *4 (D. Nev. Jan. 6, 2017) (striking terms which were inflammatory). "Language that serves no purpose and encourages a jury to draw inferences that a defendant was involved in collateral activities irrelevant to the count may be stricken." *United States v. Trie*, 21 F. Supp. 2d 7, 20-21 (D.D.C. 1998) (citation and internal punctuation omitted); *see United States v. Braunm*, No. 3:18-CR-30-TAV-DCP, 2018 WL 4560356, at *2 (E.D. Tenn. Aug. 20, 2018) ("Rule 7(d) is properly invoked when an indictment contains nonessential allegations that could prejudicially impress the jurors."). "Whether to strike surplus language from an indictment is a matter within the sound discretion" of the Court. *Braunm*, 2018 WL 4560356, at *2. Here, the crypto mining allegations in Count 1 are prejudicial and inflammatory surplusage that should be stricken by the Court.

Count 1 is addressed in 22 paragraphs of the Indictment. Dkt. No. 102 at 1-5. Of those 22 paragraphs, 21 are devoted to the primary thrust of the government's wire fraud allegations—that Ms. Thompson "exploit[ed] the fact that certain customers of [AWS] had misconfigured web application firewalls" with the object of "us[ing] that misconfiguration to obtain credentials for accounts of those customers . . . to view and



**FEDERAL PUBLIC DEFENDER**
**1601 Fifth Avenue, Suite 700**
**Seattle, WA 98101**
**(206) 553-1100**

copy data stored by the customers." *Id.* Only a single paragraph, Paragraph 21, discusses the notion that it "was further part of the scheme and artifice that" Ms. Thompson "used her unauthorized access to certain victim servers . . . to "mine" cryptocurrency for her own benefit[.]" *Id.* at 5. This allegation is included as part of Count 1 not because it is relevant or material to the government's allegations of wire fraud—it is plainly not—but to impermissibly (and prejudicially) confuse the jury regarding the elements of wire fraud. The Court should thus strike from Count 1 all references to crypto mining (Paragraph 21).

To be clear, the allegation that Ms. Thompson utilized the purported victims' computer systems for the mining of cryptocurrency has *no bearing* on whether she utilized misconfigurations in the victim's web application firewalls to access stored data without authorization. One has nothing to do with the other. The sole crypto mining allegation in Count 1, at best, is a "collateral activit[y] irrelevant to" Count 1. *Trie*, 21 F. Supp. 2d at 20-21. At worst, it is the government's attempt to prove the intent required to substantiate a wire fraud conviction through a back door.

At trial, the government must prove beyond a reasonable doubt that Ms. Thompson intended to both "deceive *and* cheat" the alleged victim(s) of her wire fraud scheme. *United States v. Miller*, 953 F.3d 1095, 1101 (9th Cir. 2020); *see also United States v. Starr*, 816 F.2d 94, 98 (2d Cir. 1987) ("[T]he deceit must be coupled with a contemplated harm to the victim."). Loss to the victim "must be an object of [wire] fraud, not a mere implementation cost or incidental byproduct of the scheme." *United States v. Yates*, 16 F.4th 256, 264 (9th Cir. 2021) (*quoting Kelly v. United States*, 140 S. Ct. 1565, 1573-74 (2020)) (internal quotation marks omitted).

Here, the wire fraud count is problematic—even if the government could prove that Ms. Thompson's "exploitation" of the misconfigurations in the victims' AWS servers—her walking through an essentially open door—was "deceit," it has little to no



**FEDERAL PUBLIC DEFENDER**
**1601 Fifth Avenue, Suite 700**
**Seattle, WA 98101**
**(206) 553-1100**

evidence that Ms. Thompson had any intent to "cheat" the alleged victims, that is, to cause any loss whatsoever, by her alleged access and copying of stored data. *See* Dkt. No. 102 at 3-5. Notably, Count 1 is lacking *any* allegation that Ms. Thompson attempted to monetize or profit from the alleged access and copying of stored data in any way whatsoever. *See Id.* at 1-5. It refers in multiple places to Ms. Thompson's alleged stealing of financial data and "valuable" PII but does not refer to a single instance in which Ms. Thompson utilized any of that data or PII for her own benefit. *See Id.* In lieu of such evidence, Count 1 makes the wholly unrelated allegation that "[t]he object also was to use the access to the customers' servers in other ways for [Ms. Thompson's] own benefit, including by using those servers to mine cryptocurrency and thereby obtain something of value." *Id.* at 3. The government should not be permitted to confuse the jury into ascribing Ms. Thompson with the intent necessary to substantiate a wire fraud charge by substituting a wholly separate intent to defraud. Rather, the government is required to prove beyond a reasonable doubt that Ms. Thompson attempted to deceive and cheat the alleged victims when she accessed and copied their data.

Moreover, the allegations of crypto mining are misleading and legally flawed. Although "[s]uccessful mining operations consume large amounts of computer power and hardware" (*Id.* at 5), assuming Ms. Thompson executed a successful crypto mining operation she only would have consumed *AWS's power and hardware*, since AWS ran the servers she allegedly accessed. The only victim of Ms. Thompson's alleged crypto mining exploits would be AWS, yet AWS is not listed as a victim in the Indictment, and the defense is aware of no evidence that Ms. Thompson's alleged crypto mining utilizing AWS servers caused any of the victims enumerated in the Indictment any damage, such as an increased invoice for usage.



**FEDERAL PUBLIC DEFENDER**
**1601 Fifth Avenue, Suite 700**
**Seattle, WA 98101**
**(206) 553-1100**

Rule 7(d) exists so that the government may not bootstrap prejudicial or inflammatory allegations that are wholly collateral to the crime charged so as to confuse the jury. *See Laurienti*, 611 F.3d at 546-47 (citation omitted). The Court should exercise its discretion to strike all references to crypto mining from Count 1 (*i.e.,* Paragraph 21), and require the government to try to prove all elements of wire fraud at trial.

**B. The Court Should Sever Count 8 Under Fed. R. Crim. P. 14(a) Because Its Inclusion Impermissibly Prejudices Ms. Thompson.**

For the same reasons the Court should strike the crypto mining allegations in Count 1, it also should sever Count 8 pursuant to Federal Rule of Criminal Procedure 14 (a) because it would impermissibly confuse the jury. Rule 14(a) provides that the Court "may order separate trials of counts" or "provide any other relief that justice requires" where joinder of offenses in an indictment "appears to prejudice a defendant." The Court may conduct an evidentiary hearing to determine whether severance is appropriate. *See* Fed. R. Evid. 104(c)(3).

Just as the government spends 21 of its 22 paragraphs devoted to Count 1 on Ms. Thompson's alleged scheme to exploit web application firewall misconfigurations to access and steal data, it alleges five counts of CFAA violations (Counts 2-7), a count of access device fraud (Count 9), and a count of aggravated identity theft (Count 10) related to the same scheme. Each of these counts is specific in that is provides facts relating to the conduct alleged (*i.e.,* the alleged victim, the data of access, the exact type of data stolen). Count 8, the singular crypto mining count, stands apart in that it is not related to the other counts in the indictment, nor does it identify particular victims ("Victim 7, Victim 8, and other victims"), dates ("on or before March 10, 2019" until "on or after August 5, 2019"), or amounts of cryptocurrency mined. Instead, it appears to serve as a "catch-all" count for allegedly malicious intent rather than part of the



**FEDERAL PUBLIC DEFENDER**
**1601 Fifth Avenue, Suite 700**
**Seattle, WA 98101**
**(206) 553-1100**

scheme alleged by the government. As such, it should be stricken and subject to a separate trial.

At a minimum, the Court should conduct an evidentiary hearing to determine whether the government intends to introduce evidence to substantiate its crypto mining charges against Ms. Thompson independently or whether it intends to use Count 8 as a stalking horse for intent on its other CFAA charges, just as it has attempted to use the crypto mining allegations in Count 1. This is necessary because the Indictment does not suggest that the charges of crypto mining, on the one hand, and unauthorized access and theft of stored data, on the other, "either depended upon or necessarily led to the commission of the other," *United States v. Jawara*, 474 F.3d 565, 574 (9th Cir. 2007) (internal quotations omitted), or were of "similar character." *Id.* at 578 (describing factors "such as the elements of the statutory offenses, the temporal proximity of the acts, the likelihood and extent of evidentiary overlap, the physical location of the acts, the modus operandi of the crimes, and the identity of the victims" as elements for consideration). Of particular note should be that the other CFAA counts in the Indictment, Counts 2-7, clearly allege that Ms. Thompson "intentionally accessed a computer without authorization." Dkt. No. 102 at 6-7. However, Count 8 does *not* allege that Ms. Thompson accessed a computer without authorization, only that she "intentionally caused damages without authorization to protected computers" by crypto mining. *Id.* at 7. This distinction is important not only because it lays bare the government's reasons for including such a count in the Indictment, but it wholly fails to allege a CFAA violation.

As outlined in Ms. Thompson's concurrently filed motion to dismiss the CFAA counts (including Count 8), a CFAA charge must allege that a defendant entered a computer system "to which a computer user lacks access privileges." *Van Buren v. United States*, 141 S. Ct. 1648, 1657-58 (2021). The motive for accessing a computer



**FEDERAL PUBLIC DEFENDER**
**1601 Fifth Avenue, Suite 700**
**Seattle, WA 98101**
**(206) 553-1100**

system is completely irrelevant for purposes of the CFAA. *See Id*. at 1652 (holding that CFAA does not impose liability for someone who has "improper motives for obtaining information that is otherwise available to them"). Assuming a person has access to a computer system, there can be no CFAA liability where that person utilizes the computer system in a way that benefits herself even if that benefit is at the expense of the computer system. *See Id.* at 1659 (describing liability as a "gates-up-or down approach").

Count 8 thus fails to allege an actual CFFA violation; rather, its presence in the Indictment appears to be solely to suggest a potential motive for Ms. Thompson's other CFAA violations. *See United States v. Midkiff*, 614 F.3d 431, 440 (8th Cir. 2010) ("[P]rejudice may result from a possibility that the jury might use evidence of one crime to infer guilt on the other or that the jury might cumulate the evidence to find guilt on all crimes when it would not have found guilt if the crimes were considered separately.") (quoting *United States v. Boyd*, 180 F.3d 967, 981-82 (8th Cir. 1999); *Davis v. Coyle*, 475 F.3d 761, 777 (6th Cir. 2007) ("[T]he jury also may confuse or cumulate the evidence of the various crimes charged."). As such, it is improper and should be stricken, or, at a minimum, the Court should require the government to proffer evidence sufficient to present to a jury of an actual CFAA violation based on Ms. Thompson's alleged crypto mining.

## IV. CONCLUSION

For all of foregoing reasons, the Court should strike the allegations regarding crypto mining from Count 1 and sever Count 8. Regarding Count 8, the Court could, in the alternative, hold an evidentiary hearing requiring the government to provide further evidence on Count 8.

/ / /

/ / /



**FEDERAL PUBLIC DEFENDER**
**1601 Fifth Avenue, Suite 700**
**Seattle, WA 98101**
**(206) 553-1100**

DATED: December 2, 2021.

Respectfully submitted,

/s/ Mohammad Ali Hamoudi
MOHAMMAD ALI HAMOUDI

/s/ Christopher Sanders
CHRISTOPHER SANDERS

/s/ Nancy Tenney
NANCY TENNEY
Assistant Federal Public Defenders

/s/ Brian Klein
BRIAN KLEIN

/s/ Melissa Meister
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson



**FEDERAL PUBLIC DEFENDER**
**1601 Fifth Avenue, Suite 700**
**Seattle, WA 98101**
**(206) 553-1100**